

**INHOPE**

# Digital Literacy Guide



Funded by  
the European Union



# Contents



## Know your Device 4

---

[Do You Update Your Phone Regularly?](#) 5

[What Does a Strong Password Look Like?](#) 5

[Is Your Location Private?](#) 5

[Is Your Phone Listening?](#) 6

[Is Your Phone Camera Safe?](#) 6

[How Do You Know Which Apps are Secure?](#) 6

[Who Can See Your Social Media?](#) 7

[How to Browse Safely?](#) 7



## Interacting Online 8

---

[Can You Make a Difference Online?](#) 9

[Why Should You Think Before You Share?](#) 9

[How to use AI Safely?](#) 9

[Safe Gaming Online](#) 11

[What is Phishing?](#) 12

[Sexting: What to Keep in Mind](#) 13

[What About Strangers Online?](#) 14



## Seeking Help 15

---

[Reaching Out for Support](#) 16

[Additional Resources](#) 17

## Why Do You Need Digital Literacy?

Technology is always changing, and it evolves faster than a TikTok trend. You might be an internet pro, but let's be real: confidently navigating the online world isn't just about knowing your way around apps. It's about creating an online space where you feel safe, connected and respected.

We know there's a lot of talk about "online safety," but it goes beyond just avoiding dodgy links or setting a strong password. It's about understanding how to protect yourself and being mindful of how we interact with others online. What if we told you that being digitally smart can make your time on the internet not only safer but also way more positive and enjoyable for you and those around you?

That's why we've put together some simple yet powerful tips. In just a few minutes, you'll learn how to avoid scams and misinformation, spot the dangers, and create an online space where you and your friends can thrive without worry. Why does this matter? Because the internet is vast, and no one is immune to online risks. The more you know, the better choices you make, and the safer everyone feels.

*But always remember: Even if you've taken all necessary steps to protect yourself, someone may still take advantage of you - whether they are someone you know or a stranger. And if someone crosses a line, it's always their fault - never yours. You deserve to feel safe, and support is always available.*





Section 01

# Know Your Device



Just like your home or room, your phone is your personal space, and keeping it secure is a must. But it's not just about protecting yourself from strangers—sometimes, people you know, like partners or friends, can overstep boundaries by accessing your phone or personal information without permission. So, how do you make sure your info and activities stay private, and your device stays safe from all threats? Start by getting the most out of your privacy and safety features to keep control over who has access to your personal space—both online and offline.



## Do You Update Your Phone Regularly?

Software updates are very important in protecting your safety online and offline. They tend to fix loopholes discovered in the previous versions and ensure that your device is equipped with the latest security measures. Cybercriminals are quick to exploit system weaknesses, so updating your software helps protect your device from unauthorised access and potential threats.



## What does a Strong Password Look Like?

Your password is your first line of defence, so it must be strong. Avoid using your birthday, known information about you or easy-to-guess combinations like "password123". [See here](#) what could happen if you are not careful. Mix it up with numbers, letters and symbols and make it at least 12 characters long. Use a different password for every account and try to keep it unpredictable. To add another layer of protection and keep your information safe even if someone cracks your password, use multifactor authentication across all your online accounts, email and social media.



## Is Your Location Private?

Your device can track where you are, and sharing your location can be useful for navigating or keeping in touch with family. But it's important to think carefully before sharing your location with friends or a partner. What might start innocently can sometimes escalate into controlling or even abusive behavior. Continuous location sharing can create a situation where someone monitors your every move, which can negatively affect your relationships and personal safety.

To protect yourself, go to your settings, find "Location," and choose which apps can access your location. We recommend only allowing apps to track you when you're actively using them and limiting location sharing overall to keep your personal space safe.

## Is Your Phone Listening?

Your device might be tuning into your audio surroundings. While enjoying music, podcasts, or using voice commands can enhance your experience, it's crucial to control who's listening. Navigate to your device settings, locate 'Audio' or 'Microphone,' and choose which apps can access your device's microphone. Be selective in giving audio permissions, allowing apps to listen only when you're actively using them. This helps you make sure that your phone is not listening to you when you least expect it.



## Is Your Phone Camera Safe?

Many apps require permission to access your camera or your gallery while you use them. While some apps need these permissions to operate, for example to share pictures, others don't. Granting camera access to suspicious apps can lead to your personal information being stolen or your device's camera being used to spy on you. To prevent this, configure your settings to limit the number of apps that have access. It's important to be vigilant about managing permissions and review them carefully before installing any app. Always prioritise your privacy and security by controlling who can access your personal information.

## How Do You Know Which Apps are Secure?

Not every app online is secure, some of them might be after your data. Before you download, it is important to check out the reviews on the App Store (iOS) or Google Play (Android). What are people saying? Any red flags you should be aware of? If the reviews are positive, great! Trust your gut if something looks suspicious.

## Who Can See Your Social Media?

Just like in real life, you control who is in your friend circle and who has access to your personal information. Your accounts are your space and you decide who gets in and who stays out. Most platforms allow you to create specific lists of people who can see your posts, so keep your private information and pictures for your inner circle and be mindful of the content you share with everyone. If you want to keep your account public, carefully consider anything you post and avoid identifying information like your home address, financial details or live location.

## How to Browse Safely ?

Always make sure you're staying on the safer side of the internet. How? Start by checking your settings and reviewing your security controls. Popular browsers offer enhanced protections that warn you about dangerous websites, and extensions. But if you want to take your browsing safety to a new level consider using privacy-focused browsers like DuckDuckGo or Qwant. These browsers are specifically designed to protect your privacy and information online.

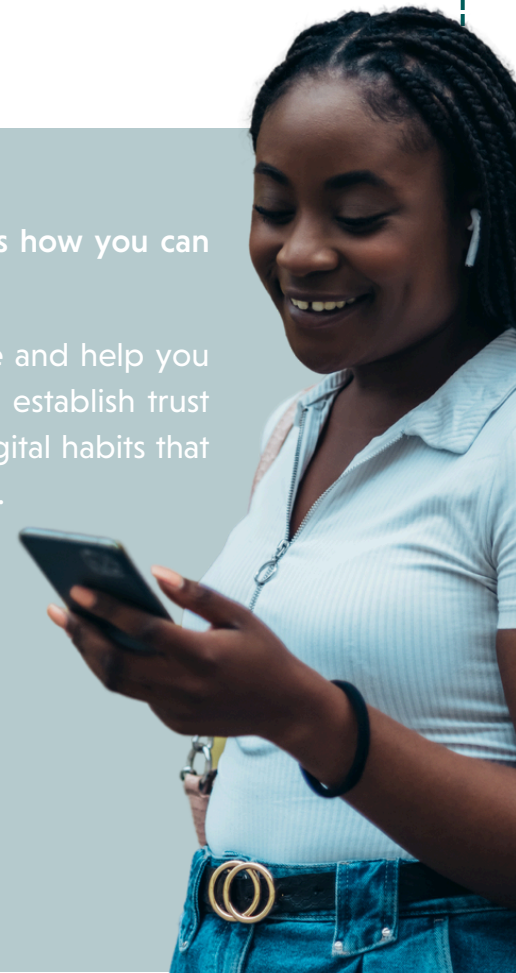
Always make sure your connection is encrypted and secure by checking for "HTTPS" in the address bar. If the website's URL does not begin with "HTTPS", think twice before using it. And especially, before sharing any private information or entering your password.

## ADVICE

Are your parents hesitant to let you have your first phone? Here's how you can address their concerns while keeping your privacy.

There are apps and tools that can improve your online experience and help you stay safe, while also respecting your privacy. These tools can help establish trust between you and your parents, but it's important to set healthy digital habits that work for you, whether or not you have that support system at home.

Apps like Qustodio, for example, offer features such as Safe Search to help filter out disturbing content and a Panic Button that lets you alert a trusted contact in emergencies. If you can't talk to your parents, think about who else you can turn to—whether it is another family member, a teacher, or a trusted adult—if something online makes you feel uncomfortable. Your safety should always come first, and support is available, even if it's not from a parent.





Section 02

# Interacting Online







## Can You Make a Difference Online?

Online interactions can be just as important as talking in person. Especially when it comes to how it makes us feel. Respectful communication creates a positive environment and builds a strong online community. Remember to stay nice when you comment or chat online. If you're feeling really angry or upset, take a few moments away from your phone or laptop to calm down. Always think before hitting send, and be mindful of the impact your words can have on others. Before saying anything harmful or insulting, consider whether you would say the same thing face-to-face.

Stepping up for others is also just as important. If you witness someone being bullied, insulted or harassed, report it. You can find more resources on how and where to report harmful things online [here](#).



## Why Should You Think Before You Share?

Anything you share online leaves a lasting footprint, so take a moment to think before you hit the share button. Ask yourself: is this content respectful, accurate, and something I have permission to share? Sharing false information can harm others, damage reputations, or even lead to legal consequences. Social media algorithms often boost controversial or sensational content, which means misinformation spreads fast and wide. So, it's worth double-checking the facts using reliable tools like [Snopes](#), [FactCheck.org](#), or [GoogleFactCheck](#). If something sounds too extreme or too good to be true, it's probably time for a fact-check.

For your own privacy and safety, always be cautious about what you share. And when it comes to others, consent is key—especially in sensitive situations. Before posting pictures or information about someone, ask if they're okay with it and respect their decision no matter what it is. If you accidentally share misinformation or harmful content, act quickly. Delete the post and set the record straight. Being mindful about what you share helps keep the online space safer and more trustworthy for everyone.



## How to use AI Safely?

Artificial Intelligence can generate images, videos, stories or voice messages on command. It can be fun to use these tools creatively but generating violent, offensive, or illegal material is bad and might have real legal consequences. For example, AI can be used to create [deepfake videos](#) that falsely show people doing things they'd never do or saying things they'd never say.

Deepfakes can trick people, cause confusion, and even permanently damage reputations or destroy relationships. So, for your own sake and in consideration of others, never create or spread any harmful AI-generated content. Always keep in mind that fake content can have a very real impact.

Today, everyone can have access to AI tools. You might have already used AI to generate a picture or help with your schoolwork. But there are also many ways in which these tools can be misused.

### How could AI be used to trick you?

- Impersonating another person through voice, image or videos.
- Creating fake nude pictures or videos (deepfakes) of you to use for blackmail.
- Generating illegal and disturbing content that might be traumatising to see.

Knowing this, it's important to be cautious about the content you encounter online and to not believe everything you see or hear. Always be critical and pay attention to signs that something might be AI-generated.



## How to spot AI-generated content?

Identifying AI-generated content can be tricky, but with a little attention, you can spot it. First, look for things that seem “off”—like overly polished images, text that feels too perfect, or odd mistakes humans wouldn’t usually make, like strange hands in photos or awkward sentence phrasing. AI tools can produce content that looks and sounds real, but sometimes it lacks the natural flow or small imperfections typical of human work.

Another tip is to fact-check. AI-generated content, especially in text, might present information that sounds convincing but isn’t accurate or verified. You can also use reverse image search tools to check if an image has been generated or altered. Be especially cautious with viral or sensational content—it might spread quickly but could be misleading or fake.

If you come across content you know is fake or misleading, don’t just ignore it—report it. Most platforms have features to flag or report false content, which helps prevent the spread of misinformation.

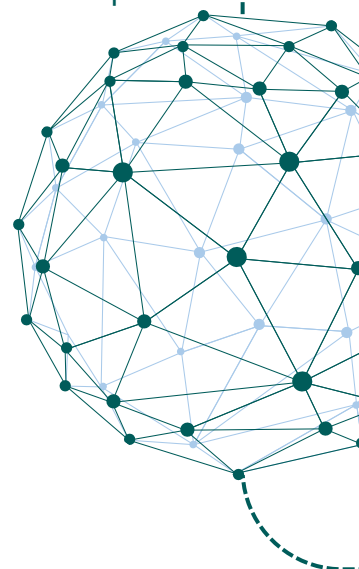


## Safe Gaming Online

Gaming is all about skills, challenges, and connecting with others who share your interests. To ensure you’re having a great time while staying safe, it’s essential to play respectfully and supportively. This means being kind to fellow players, playing fairly, and respecting everyone’s contributions. Encouraging a positive and inclusive gaming environment makes the experience better for everyone.

However, not everyone you meet online will play fair. Keep your guard up, be aware of potential red flags, and don’t trust too easily. Keep personal details like your real name, address, or school private. If someone in the chat is making you uncomfortable, log out or mute them. Your safety is the top priority, so don’t hesitate to block or report toxic players.

Remember, discrimination can occur in gaming communities, and individuals from marginalised groups are often targeted. It’s important to look out for each other and offer support, especially to those who might be more vulnerable. If you experience or witness discriminatory behaviour or harassment, speak up and seek help. Talk to someone you trust, whether it’s a friend, family member, or a counsellor. By standing together and addressing issues as they arise, we can create a more positive and inclusive gaming environment for everyone.



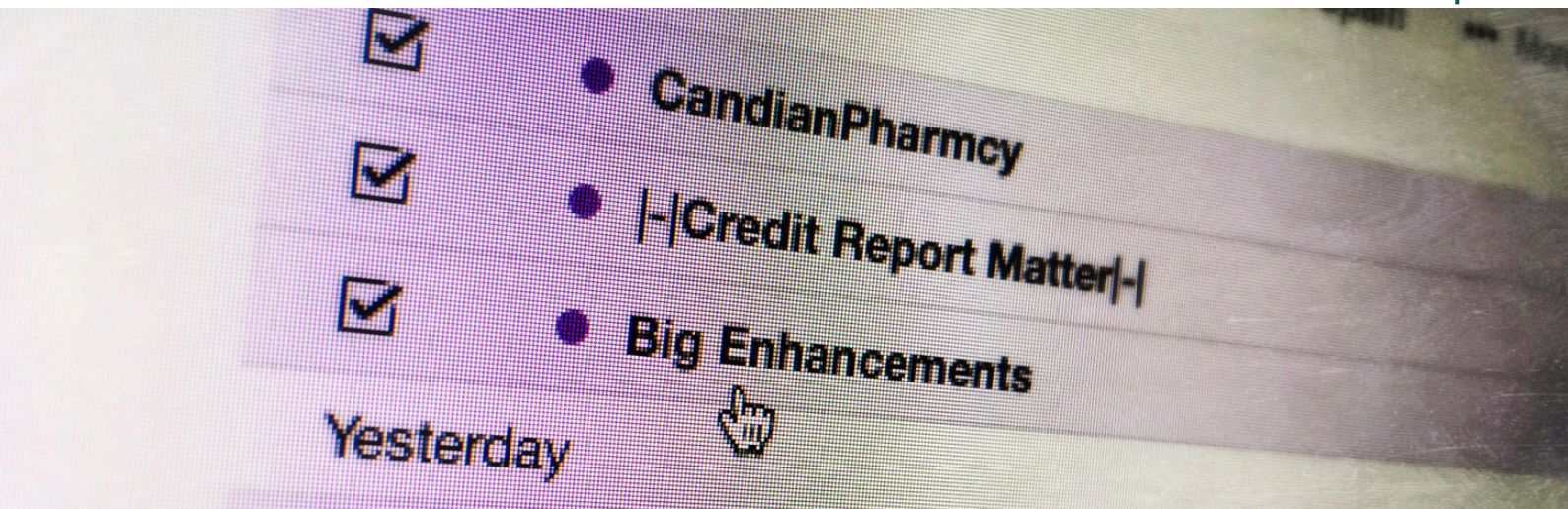


## What is Phishing?

Phishing is a fraudulent practice where scammers pretend to be a trusted company or person to trick you into sharing your personal info or passwords. Phishers use emails, messages, or fake websites to trick you. They may pretend to be a friend in need asking for a favour or a reputable company claiming you have won a prize.

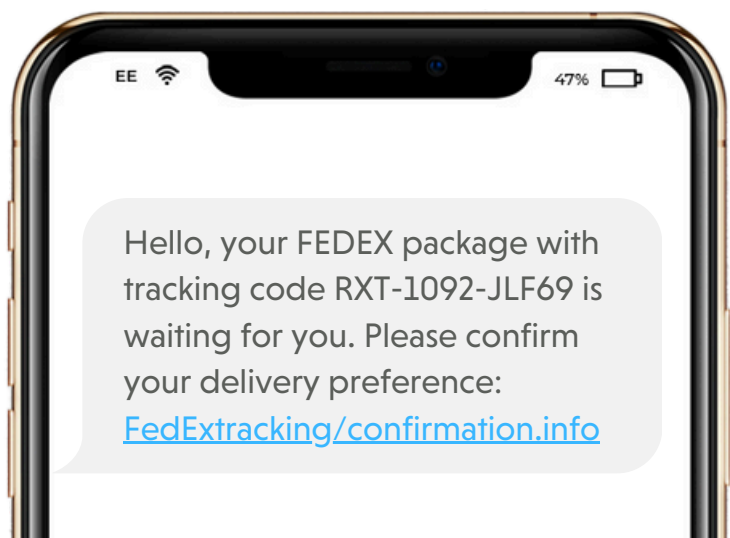
### Be cautious of:

- Urgency, as scammers often create a sense of panic to prompt quick action.
- Generic greetings that don't use your name.
- Misspelt URLs or slight variations in a company's name.
- Unexpected prizes or gifts that can be 'claimed' through a link.



Clicking on phishing links isn't just a danger to your device; it can lead to malware, identity theft, or unauthorised access to your accounts. So, when it comes to clicking on links, think about your safety. Carefully preview the link's URL. If it looks off or is misspelled, don't click. Always verify the source of emails, messages and the safety of websites before taking any action.

Text-based phishing, also called 'smishing,' is particularly common and can appear as urgent messages from familiar contacts or companies, asking you to click on a link or provide personal details. Always be cautious if you receive a message you were not expecting. Particularly if it claims to be from a family member in need.





## Sexting: What to Keep in Mind

Flirting over text and sending nude pictures can be a natural part of exploring your sexuality and connecting with people. Many young people and adults have experience with sexting, and when it is done with consent and respect for everyone involved it can be a positive experience. But there are important things to keep in mind, before you jump into sending your first nude or sext.

### CONSENT

Everyone involved should be totally cool with sexting. If either of you is not okay with it, stop right there. You can change your mind at any time.

### COMMUNICATION

Talk clearly about your expectations. Agree on your boundaries and discuss how you will safeguard the images and messages you exchange.

### REFLECTION

Regularly reflect on your feelings about sexting. If you start having doubts about it you should be comfortable to stop at any time.

Sexting can only be safe and positive when everyone involved is completely comfortable with it at all times. Never show or share private messages with anyone else and make sure you are keeping any private content secure and inaccessible to others.

## Sexting Abuse

Sexting is meant to be private, but sometimes things don't go as planned. Whether by accident or on purpose, if someone shares or forwards your private images without your consent, it's called sexting abuse. This is illegal and never your fault—the responsibility lies entirely with the person who shared your image without permission. If this ever happens to you, it's normal to feel angry, devastated, or embarrassed. But always remember, you're not alone, and you are not to blame!

There are free services available worldwide to help you through situations like this. You can reach out to a [helpline](#) for emotional support, advice, or tips on how to get your images removed from the internet as quickly as possible.

If someone threatens to share your private messages or images, it's called sextortion. This often involves demands for money, services, or more explicit content in exchange for keeping your images private. This can feel incredibly stressful and overwhelming, but remember, you are never at fault. Help is always available, and there are experts ready to support you. [Find resources and support.](#)



## What About Strangers Online?

Making friends online is common, and it often feels like you've known them forever. But what if your online friend isn't who they claim to be? If they start asking for private details or turning the conversation sexual, you might be dealing with a groomer.

Groomers are adults who pose as friends online to gain your trust and manipulate you into a sexual relationship. They are experts at deception, making it difficult to detect their true intentions. Remember, it is never your fault if you fall for their tactics—groomers deliberately exploit trust and friendship. While anyone can be targeted by a groomer, there are people who are more vulnerable to this abuse, like people part of the LGBTQ+ community.

Watch out for red flags like requests to keep your online relationship a secret; this can be a sign of manipulation or control. Healthy and respectful relationships should not require secrecy. Real friends don't lie or pressure you into anything you're uncomfortable with. If you're unsure about someone's identity, avoid sharing personal details and try to verify what they tell you. If you plan to meet someone you met online, always inform your parents and bring a trusted friend.

### What Should You Look Out For?

Just like in real life, it's important to be aware of anything online that doesn't feel right. Some people may try to pressure you into things you're not comfortable with, whether through cyberbullying, harassment, or sending unwanted pictures, or through more subtle manipulation. Remember, all of this behaviour is harmful and unacceptable. Trust your instincts—report it and seek support if needed.

## ADVICE

Watch out for sudden changes in your friends' behaviour, such as withdrawal, secrecy, or being overly glued to their devices—these could be signs that they're struggling online. If you sense something might be wrong, be the friend who starts the conversation. Approach them with empathy and let them know it's okay to open up without fear of judgment.

You can start by saying something like, "I've noticed you seem a bit off lately. If you want to talk, I'm here for you. Your support can make all the difference, so make it clear that it's safe for them to share their experiences and that they won't get in trouble for being honest."





Section 03

# Seeking Help





## Reaching Out for Support



Your safety and well-being are a top priority. If you are being bullied, blackmailed, extorted, or if your private pictures are leaked online, don't hesitate to talk to someone you trust—whether it's a friend, family member, teacher, or counsellor. Remember, a counsellor is bound by confidentiality and is there to help you without judgement. You are never alone in facing these challenges. Many others have gone through similar struggles, and numerous organisations are dedicated to offering the support you need. If you're in a difficult or harmful situation, know that help is always available.

### Reach out to Helplines



Online threats can leave you feeling overwhelmed, confused or scared – and that is normal. Reaching out to a helpline can provide a safe and confidential space to talk about your concerns or help you through your situation. You can call, text or chat with them online for free. Find your local helpline [here](#).

### Report Toxicity on Social & Gaming Platforms



Socials should be a safe space to interact with your friends, express yourself and be creative. If you come across something that feels off – whether it's inappropriate content or someone behaving in a harmful way – report it. Most social, and gaming platforms have a reporting feature. Find it in the settings or options menu and let them know what is going on.

### Report Harmful Content to Your Hotline



Hotlines work to rapidly remove online sexual abuse material from the internet. If your intimate content has been leaked online or if you ever come across intimate material involving children, report it. Our network of hotlines operates across all continents and our analysts are specifically trained to handle these situations. Find your local hotline [here](#).



## Take **It** Down

Take it Down Tool: If you are over 18 and had an intimate image leaked online before turning 18, the Take it Down Tool can help you protect your privacy by having your content removed from the internet.

Do you want to learn more about how to keep yourself safe online? Then find your local Safer Internet Centre [here](#). This platform offers safety tips, resources, guidance and advice on how to have a safer online experience.



## References

- [5 Reasons software updates are important](#)
- [App permissions explained: Which ones should you allow?](#)
- [6 Tips to know if an app is safe](#)
- [How bad actors access webcams and other cameras](#)
- [Secret Selfies: Can Phones Take Pictures and Videos of You Without Your Knowledge?](#)
- [Location Services: A Quick Guide for iPhone and Android](#)
- [Family Sharing - Share your favourite things with your favourite people](#)
- [5 Best Parental Controls for Teenagers in 2024](#)
- [Best private search engines that won't track you in 2024](#)
- [Share with Care: Staying Safe on Social Media](#)
- [How to Recognise and Avoid Phishing Scams](#)
- [Bullying, a guide for young people](#)
- [Child Safety in Gaming](#)
- [What is self-generated CSAM?](#)
- [The impact of online grooming](#)
- [5 ways to Protect Yourself from Sexual Abuse Online](#)
- [Support and Safety through Helplines](#)

*Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency. Neither the European Union nor the European Education and Culture Executive Agency can be held responsible for them.*

# INHOPE

A Digital Literacy Guide for young people, caretakers, teachers and hotlines.

Learn more and support us at [inhope.org](http://inhope.org)



Funded by  
the European Union

